REMARKS

Applicants respectfully request reconsideration and allowance of the above-identified patent application. By this paper, claims 1-28 and 41-43 remain pending by canceling claims 29-40 and adding new claims 41-43.[1] Note that the independent claims of those pending include claims 1, 10, 19, 24, and 41.

Initially, Applicants and Applicants' Attorney express appreciation to the Examiner for allowing the telephonic communication presented on January 22, 2008. The foregoing amendments and following arguments are consistent with those presented during the communication.

Applicants also note with appreciation the Examiner's consideration of the documents submitted in the Information Disclosure Statement (IDS) filed December 12, 2003.

The Office action rejects the claims under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent Application Publication No. 2004/0198220 to Whelan et al. ("*Whelan*").[2] Applicants respectfully traverse this ground of rejection.

Applicants' invention generally relates to secure verification of network communications, especially in a wireless and/or wired networking environment with continuous network connection requests and/or connection transfers. Existing network technologies involve the potential for a hack to maliciously broadcast false requests and false information about its capabilities, which can cause such problems as undesirable termination of an existing connection, unauthorized associations with a network, or other similar attacks. Such undesirable network security threats are more commonly known by such terms as spoofing, network hijacking, data packet forging and modification, resource starvation attacks, impersonation, and so forth.

---

[1] Support for the claim amendments can be found throughout the specification; for example, support may be found in the following paragraphs: [0046]—[0052].

Applicants further note that the cancelation of various claims from those originally filed have been made in order to focus the subject matter in this application and reduce issues raised by the Office. Such amendments; however, should not be construed as Applicants' acquiescence to any assertions made by the Office regarding the patentability of such claims and Applicants reserve their right to challenge such allegations in any future correspondences for this or any subsequently filed related applications.

[2] Although the prior art status of the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status of the cited art at any appropriate time, should it arise. In fact, Applicants note that the filing date of *Whelan* predates Applicants' priority date by less than one year, and may not qualify as prior art. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

Although available techniques have been implemented to improve the security of networks by requiring that network devices be authenticated by the network prior to being granted access, this mechanism still fails to resolve the above problems. For example, a resource starvation attack could still occur when the capabilities of a network access point are publicized incorrectly by a hack. In such an instance, the network access point appears so attractive that all or a large number of devices in the serviceable range of the access point choose to access the network through that single access point rather than other available access points. In other words, simple authentication of an access point to a device in a wireless network does not provide for adequate assurance against all types of network service attacks.

Embodiments herein overcome the foregoing problems by not only providing unique mechanisms of authentication for an access point, but also verification of discovery information thereof. As with typical systems, capabilities of various access points are broadcast or otherwise made available to stations (e.g., cell phones, PDAs, personal computers, and other wireless/wired devices). Such information is received by the station in the form of "discovery information" to determine which of the access points have the best capabilities for facilitation of the desired network communications. For example, different access points might provide different signal strengths, transfer rates, security features, available channels, restrictions, and so forth. Accordingly, such information is used in determining an appropriate access point to connect with.

Upon selecting an appropriate or desired access point, the station authenticates the access point to validate the access point belongs to the network. For example, one embodiment authenticates the access point by identifying a certificate generated by a network authentication server or other authentication services, which was attached to the discovery information. Rather than just merely authenticating an access point, however, embodiments also engage the station in verifying the discovery information of the selected access point to ensure correctness. Accordingly, this embodiment provides the station confidence of the access point's capabilities when creating a secure associate between the station and the access point for communication purposes on the network.

For example, the station may send the discovery information back to the access point for verification along with a key, hash number, certificate, or other identifiable security object obtained during authentication or broadcast of the discovery information. The access point then

verifies the discovery information by sending an acknowledgement receipt back to the station that includes the identifiable security object. Such verification of discovery information provides for additional assurances against spoofing, network hijacking, impersonation, and other similar attacks.

Note that the above use of specific examples for verifying the discovery information is for illustrative purposes only. As such, the above description should not be used to construe or otherwise limit Applicants' claim language unless otherwise explicitly stated or claimed.

Claim 1 is directed toward some of the above described embodiments and recites a method for creating a secure association between a station and an access point comprising: (1) obtaining discovery information from access point(s) in the communications network, the discovery information reflecting capabilities of the respective access point(s) to facilitate communication with the station; (2) selecting one of the access point(s) to become associated with; (3) authenticating the selected access point; (4) sending a discovery verification request to the selected access point for the discovery information of the selected access points to be verified; and (5) receiving an acknowledgement receipt from the selected access point verifying the discovery information.

Applicants respectfully submit that the cited *Whelan* reference does not render claim 1 unpatentable for at least the reason that the cited reference does not disclose (or suggest) each and every element of Applicants' claimed invention.[3] For example, *Whelan* does not disclose both authentication of an access point and verification of discovery information thereof, as recited, *inter alia*, in claim 1.

Whelan discloses management of mobile units in a roaming environment. Although *Whelan* provides for enforcement of additional policies beyond mere authentication of an access point, *Whelan* does not provide for verification of access point discovery information. More specifically, *Whelan* authenticates the access points to ensure both authorization and

[3] "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131. That is, "for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly." MPEP § 706.02. Applicant also note that "[i]n determining that quantum of prior art disclosure which is necessary to declare an applicant's invention 'not novel' or 'anticipated' within section 102, the stated test is whether a reference contains an 'enabling disclosure.'" MPEP § 2121.01. In other words, a cited reference must be enabled with respect to each claim limitation.

management thereof by providing the mobile units with a "list" of access points it may and/or may not associate with. (*See e.g.*, the abstract and other cited sections noted in the Office action). For example, the lists may provide for one or more of the following: a set of mandatory access points; a set of preferred access points, but allowing association with other access points; a set of exclusion or no contact access points; etc. The simple use of an access list, however, does not disclose (or suggest) both authentication of a specific access point and verification of its discovery information as currently claimed. In fact, *Whelan* suffers from similar deficiencies as other networking systems noted above.

More specifically, the list of *Whelan* simply identifies if an access point discovered is part of a managed network, which if approved (based on the list provided) it then authenticates through standard mechanisms. *Whelan*, however, is silent with regard to validating or verifying discovery information used in selecting the access point in the first place. Accordingly, the white and black list provided by *Whelan* merely prevents the connection of a mobile unit to unmanaged or undesired access points, but does not go far enough to ensure accuracy of the discovery information used to connect to authorized or managed points. In other words, just because an access point appears on a "mandatory" or "preferred" list, does not ensure the correctness of the discovery information used to access it. As such, hacks may still hijack a system using false information to entice many mobile units to connect to a managed access point (which may: not have such capabilities; not necessarily be the desired access point; cause a denial-of-service attack; or have many other undesired results).

Since *Whelan* does not disclose (or suggest) both authentication of an access point and verification of discovery information thereof, *Whelan* does not render claim 1 anticipated. In fact, because *Whelan* discloses a separate mechanism for combating hack attacks (i.e., the use of white and black lists), *Whelan* actually "teaches away" from Applicants' claimed invention for verification of access point discovery information. As such, Applicants respectfully submit that *Whelan* should not be used in combination with any other references in an attempt to reject Applicants' claimed invention in future communications received from the Office.

Independent claims 10, 19, 24, and 41 recite methods and computer program products with elements similar to those described above with regard to the distinctions of claim 1 over the cited *Whelan* reference. As such, these claims are patentably distinct over the cited art of record for at least those reasons stated above with regard to claim 1.

Based on at least the foregoing reasons, Applicants respectfully submit that the cited prior art fails to anticipate or otherwise make obvious Applicants' invention as claimed in the independent claims. Applicants note for the record that the remarks above render the remaining rejections of record for the independent and dependent claims moot, and thus addressing individual rejections or assertions with respect to the teachings of the cited art is unnecessary at the present time, but may be undertaken in the future if necessary or desirable and Applicants reserve the right to do so.

All objections and rejections having been addressed, Applicants respectfully submit that the present application is in condition for allowance, and notice to this effect is earnestly solicited. Should any questions arise in conjunction with this application or should the Examiner believe that a telephone conference with the undersigned would be helpful in resolving any remaining issues pertaining to this application, the undersigned respectfully requests that he be contacted at 1-801-533-9800.

DATED this 22nd day of January, 2008.

Respectfully Submitted,

/Wesley C. Rosander, Reg.# 51,030/
Wesley C. Rosander

RICK D. NYDEGGER
Registration No. 28,651
WESLEY C. ROSANDER
Registration No. 51,030
Attorneys for Applicant
Customer No. 047973

RDN/WCR:crb
W:\13768\432.1\CRB0000008117V001.doc